TECHNICAL LIBRARY
CONTRACTOR INVESTIGATIVE REPORTS (CIR) FOR IT ACCESS

SECTION 1   INITIAL REQUESTS

Step 1.   Contractor shall complete and submit Contractor Investigative Report (CIR) to CGA Security POC who reviews to ensure appropriate information has been completed to include required signatures.

Step 2.   Contractor shall submit DD 2875 (SAAR) (1 or 2 forms may be submitted based on systems access requirements) with parts I and III completed to include required signatures to CGA Security POC. (If employee currently has logon, it should be annotated on the DD 2875 and still processed as an initial request.)

Step 3.   CGA Security POC provides completed documentation to DDC Security Office.

Step 4.   DDC Security office conducts appropriate checks to determine if the individual is eligible.

1.1   IF ELIGIBLE:

Step 1.   DDC Security Office completes contractor investigative request (CIR) and returns it to the CGA Security POC.

Step 2.   CGA Security POC completes Part II of DD 2875(s) and faxes to DDC J-6.

Step 3.   DDC J-6 obtains required systems access and forwards information to CGA Security POC.

Step 4.   CGA Security POC coordinates with CGA TASO and provides information to Contractor.

1.2   IF NOT ELIGIBLE:

Step 1.   DDC Security Office sends notification thru CGA Security POC to the contractor specifying what the requirements are to initiate an investigation.

Step 2.   Contractor has employee complete appropriate form(s).

Step 3.   Completed form(s) are routed to CGA Security POC for review.

Step 4.   CGA forwards form(s) to DDC Security

Step 5.   DDC Security reviews form(s). Investigation is submitted to the appropriate investigative agency.

Step 6.   If information is favorable, DDC Security will advise the CGA Security POC that a waiver may be requested

Step 7.   If information is not favorable, a waiver cannot be done and DDC Security Office notifies CGA security who notifies the Contractor.

Step 8.   Positions requiring **IT** **III** **only** may be brought on board after the investigation has been initiated. No waiver is required.

TECHNICAL LIBRARY
CONTRACTOR INVESTIGATIVE REPORTS (CIR) FOR IT ACCESS

NOTE: If a clearance is required in addition to IT access, the following guidelines will apply:

1.3   IT I or II <u>WITH</u> Clearance:

Step 1.   The Contractor shall submit request(s) for clearance to their Facility Security Officer (FSO). The FSO belongs to the contractor so the request for clearance needs to go directly from the Contractor to the FSO.

Step 2.   The Contractor shall complete the CIR and submit to the CGA Security POC indicating IT requirement.

    a.   The Contractor shall annotate on CIR that the appropriate investigation (SSBI or NACLC) for clearance was initiated or DISCO Form 562 was generated.

    b.   The Contractor shall provide a completed, signed copy of the SF 86, EPSQ receipt or a copy of DISCO Form 562 and proof of citizenship with the CIR to the CGA Security POC.

Step 3.   The CGA Security POC forwards the CIR package to the DDC Security Office.

Step 4.   Upon receipt of the CIR package, DDC Security Office reviews to determine if a waiver can be requested.

    c.   If information is favorable, DDC Security Office will advise the CGA Security POC that a waiver may be requested for the IT access.

    d.   If information is not favorable, a waiver cannot be done and the DDC Security Office notifies the CGA Security POC who notifies the Contractor.

Step 5.   If the Contractor employee is eligible for a waiver, the CGA Security POC completes the DD 2875 and faxes it to DDC J-6.

Step 6.   Upon receipt of the DISCO Letter of Consent (LOC), the Contractor shall provide a copy of the DISCO LOC to the KO or designee. The CGA Security POC will forward the LOC to the DDC Security Office to confirm the investigation has been completed and clearance was granted by DISCO.

Step 7.   Contractor FSO should ensure individuals with clearance have signed an SF 312, Classified Information Nondisclosure Agreement as specified in the National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22-M, 3-105.

1.4   IT III <u>WITH</u> Clearance:

Step 1.   The Contractor shall submit the request for clearance to the Facility Security Officer (FSO).

    a.   The Contractor shall complete and submit the CIR(s) to the CGA Security POC indicating IT requirement(s).

b.   The Contractor shall annotate on the CIR(s) that NACLC investigation for clearance was initiated or that a DISCO Form 562 was generated.

c.   The Contractor shall provide the EPSQ receipt or a copy of the DISCO Form 562 and proof of citizenship with the CIR to the CGA Security POC.

Step 2.   The CGA Security POC will forward the CIR package to the DDC Security Office.

Step 3.   Upon receipt of the CIR package, DDC Security Office reviews and advises the CGA Security POC that individual is IT III eligible.

Step 4.   The CGA Security POC completes DD 2875 and faxes it to DDC J-6

Step 5.   Upon receipt of the DISCO LOC, the Contractor shall provide a copy of the DISCO LOC to the CGA Security POC, who will forward it to the DDC Security Office to confirm investigation has been completed and clearance was granted by DISCO.

Step 6.   Contractor FSO should ensure individuals with clearance have signed an SF 312, Classified Information Nondisclosure Agreement as specified in the National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22-M, 3-105.

SECTION 2 SUBSEQUENT REQUESTS FOR ADDITIONAL IT ACCESSES

Step 1.   The Contractor shall submit subsequent requests to the CGA KO or designee.

Step 2.   The CGA TASO coordinates information with CGA Security POC; completes Part II with information previously received on CIR; and faxes to DDC J-6 as required.

Step 3.   DDC J-6 obtains required systems access and forwards information to CGA TASO.

Step 4.   The CGA TASO provides information to the Contractor.